UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,921	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.001	9480

67419 7590 07/10/2007
COATS & BENNETT/IBM
1400 CRESCENT GREEN
SUITE 300
CARY, NC 27518

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
07/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/458,921	PEYRAVIAN ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-28 and 47-50* is/are allowed.

6)☒ Claim(s) *29-46,51 and 52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 9 November 2006.

2. Claims 1-52 are pending in the application.

3. Claims 29-46, 51 and 52 have been rejected.

4. Claims 1-28 and 47-50 have been allowed.

Response to Arguments

5. Applicant's arguments filed 9 November 2006 have been fully considered but they are not persuasive.

On page 2, the applicant argues that Pasieka does not employ the secret key as input into a one-way hash function.

The examiner agrees that Pasieka does not employ the secret key as input into a one-way hash function. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., employ the secret key as input into a one-way hash function) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant argues that there is no motivation to combine Pasieka with Schneier.

The examiner respectfully disagrees. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Schneier describes how symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks [page 216].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 29-46, 51 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pasieka U.S. Patent No. 6,587,945 B1 in view of Applied Cryptography (hereinafter Schneier).

As to claim 29, Pasieka discloses a method for time stamping a document comprising:

a. receiving a time stamp request at an outside agency at a first time, the time stamp request including identifying data associated with the document [column 5 line 4 to column 6 line 14];

b. creating at the outside agency a time stamp receipt based on the identifying data and a time indication [column 5 line 4 to column 6 line 14]; and

c. generating at the outside agency a message authentication code based on the time stamp receipt and a public key [column 5 line 4 to column 6 line 14]; and

d. transmitting the time stamp receipt and the message authentication code to the requestor [column 5 line 4 to column 6 line 14].

Pasieka teaches that the message authentication code is based on the time stamp receipt and a public key, not a secret key.

Schneier teaches the benefits of asymmetric (secret) key system over a public key system [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka so that the message authentication code would have been based on the time stamp receipt and a secret key, not a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka by the teaching of Schneier because symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks [page 216].

As to claim 30, Pasieka teaches that the identifying data comprises a digital representation of at least a portion of the document [column 5 line 4 to column 6 line 14].

As to claim 31, Pasieka teaches that the identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of the document [column 5 line 4 to column 6 line 14].

As to claim 32, Pasieka teaches that the digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of the document [column 5 line 4 to column 6 line 14].

As to claim 33, Pasieka teaches that the time stamp receipt includes a copy of at least a portion of the identifying data concatenated with the time indication [column 7, lines 10-29].

As to claim 34, Pasieka teaches that the time stamp receipt includes a digital sequence derived from the identifying data concatenated with the time indication [column 7, lines 10-29].

As to claim 35, Pasieka teaches that the time stamp request further includes an identification number associated with the requestor [column 8, lines 31-49].

As to claim 36, Pasieka teaches that the message authentication code comprises a numeric representation generated by application of a deterministic function to the time stamp receipt and the secret key concatenated together [column 7, lines 10-29].

As to claim 37, Pasieka teaches generating a second message authentication code based on the first message authentication code and a second secret key [column 7, lines 10-29].

As to claim 38, Pasieka teaches transmitting the second message authentication codes to the requestor [column 7, lines 10-29].

As to claim 39, Pasieka teaches the step of encrypting the first secret key to generate an encrypted key [column 9, lines 1-21].

As to claim 40, Pasieka teaches transmitting the encrypted key to the requestor [column 9, lines 1-21].

As to claim 41, Pasieka discloses a method for time stamping documents comprising:

a. receiving at an outside agency a certification request, the certification request including a time stamp receipt and a message authentication code generated on the time stamp receipt [column 5 line 4 to column 6 line 14];

b. validating the message authentication code at the outside agency using a public key [column 5 line 4 to column 6 line 14];

c. certifying the time stamp receipt if the message authentication code is valid using a cryptographic signature scheme [column 5 line 4 to column 6 line 14].

Pasieka teaches that the message authentication code is based on the time stamp receipt and a public key, not a secret key.

Schneier teaches the benefits of asymmetric (secret) key system over a public key system [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka so that the message authentication code would have been based on the time stamp receipt and a secret key, not a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka by the teaching of Schneier because symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks [page 216].

As to claim 42, Pasieka teaches that the step of certifying the time stamp receipt includes signing the message authentication code at the outside agency using a cryptographic signature scheme [column 9, lines 41-52].

As to claim 43, Pasieka teaches that the step of certifying the time stamp record includes signing the time stamp receipt at the outside agency using a cryptographic signature scheme [column 9, lines 41-52].

As to claim 44, Pasieka teaches including the step of transmitting the certified time stamp receipt to the requestor [column 9, lines 41-52].

As to claim 45, Pasieka teaches that certifying the time stamp receipt at the outside agency comprises signing the time stamp receipt with a private signature key [column 9, lines 41-52].

As to claim 46, Pasieka teaches that certifying the time stamp receipt at the outside agency comprises signing the message authentication code with a private signature key [column 9, lines 41-52].

As to claims 51 and 52, the combination teaches that the secret key used to generate the message authentication code at the outside agency comprises a secret key of the outside agency [column 9, lines 41-52].

Allowable Subject Matter

7. Claims 1-28 and 47-50 are allowed.

As to claim 1, prior art does not disclose or fairly teach e. receiving a certification request at the outside agency at a second time, the certification request including the time stamp receipt and the message authentication code. Prior art does not disclose or fairly teach f. validating the message authentication code at the outside agency using the secret key. Prior art does not disclose or fairly teach g. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the message authentication code is valid.

As to claim 15, prior art does not disclose or fairly teach d. encrypting the first secret key with a second secret key to generate a key message. Prior art does not disclose or fairly teach e. generating a second message authentication code based on the first message authentication code and the first secret key using a third secret key. Prior art does not disclose or fairly teach f. transmitting the time stamp receipt, the first message authentication code, the second message authentication code, and the end key message to the requestor. Prior art does not disclose or fairly teach g. receiving at the outside agency at a second time a certification request, the certification request including the time stamp receipt, the first message authentication code, the second message authentication code, and the encrypted key message. Prior art does not disclose or fairly teach h. decrypting at the outside agency the encrypted key message to recover the first secret key. Prior art does not disclose or fairly teach i. validating the second message authentication code at the outside agency using the third secret key. Prior art does not disclose or fairly teach j. validating the first message authentication code at the outside agency using the first secret key if the second message authentication code is valid. Prior art does not disclose or fairly teach k. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the first message authentication code is valid.

Any claims not directly addressed are allowed on the virtue of their dependency.

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
July 4, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100